UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,916	06/24/2003	Jari T. Malinen	59864.00838	4349

32294 7590 10/14/2008

SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-6212

EXAMINER	
MATTIS, JASON E	

ART UNIT	PAPER NUMBER
2416	

MAIL DATE	DELIVERY MODE
10/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/603,916	MALINEN ET AL.	
	Examiner	Art Unit	
	JASON E. MATTIS	2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17 and 19-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-17 and 19-21* is/are rejected.

7)☒ Claim(s) *6* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed 6/26/08. Claim 18 has been cancelled. Claims 1-17 and 19-21 are currently pending in the application.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 11-13 and 15-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 11 recites the limitation “the firewall” in line 1. Claim 1 mentions “a first firewall” and claim 10 mentions “a firewall”. It is unclear whether “the firewall” in claim 11 refers to the “first firewall” of claim 1 or the “firewall” of claim 10.

Claims 12 and 13 are also rejected since they depend on rejected claim 11.

Claim 15 recites the limitation "the mobile node" in line 3. There is insufficient antecedent basis for this limitation in the claim, since there is no prior mention of “a mobile node" in the claim. It is recommended that the claim be amended such that there is proper antecedent basis for the term “the mobile node”.

Claims 16 and 17 are also rejected since they depend on rejected claim 15.

Claim Objections

4. Claims 5, 6, and 19 are objected to because of the following informalities:

Claim 5 contains a duplicate limitation from claim 1. Both claims state "wherein the mobile node has a permanent address in a known range". It is recommended that this limitation be removed from claim 5.

Claim 6 contains a duplicate limitation from claim 6. Both claims state "a demilitarized zone located outside the secure network, wherein the virtual private network gateway and the home agent reside in the demilitarized zone; a first firewall between the secure network and the demilitarized zone". It is recommended that this limitation be removed from claim 6.

Line 22 of claim 19 contains the term "a firewall". Lines 23-24 of claim 19 contain the term "the first firewall". Since "the first firewall" seems to refer back to "a firewall" it is recommended that "the first firewall" be changed to "the firewall" in order to keep the claim language consistent. Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 15-17 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adrangi et al. (U.S. Application 10/323486) in view of Liu et al. (U.S. Publication US 2004/0120295 A1 hereafter referred to as Liu et al. '295).

With respect to claim 15, Adrangi et al. discloses a method for secure communication **(See the abstract of Adrangi et al. for reference to a method providing secure mobile roaming)**. Adrangi et al. also discloses establishing a Proxy Home Agent located within the secure network to monitor data directed to a mobile node **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 300, which is a Proxy Home Agent providing Mobile IP Home Agent functionality, located within the corporate intranet 100)**. Adrangi et al. further discloses a mobile node associated with a home network in a secure network and a corresponding node **(See page 2 paragraphs 20-22 and Figure 3 of Adrangi et al. for reference to a mobile node 140 having an interface to communicate with other nodes, including CN 310, belonging to corporate intranet 100, which is a home network for mobile node 140 and is also a secure network)**. Adrangi et al. also discloses establishing a Home Agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 305, which provides Mobile IP Home Agent functionality, located outside the corporate intranet 100, for reference a mobile node creating a single security association, an IPSec tunnel, and for reference to a mobile node having one mobility bind, the**

care-of address COAx, which is the mobile node's address on the external network). Adrangi et al. further discloses collecting data directed to the mobile node **(See page 2 paragraph 20 to page 3 paragraph 25 of Adrangi et al. for reference to both home agent 300 and home agent 305 being used to collect and route data directed to the mobile node 140)**. Adrangi et al. also discloses packaging the collected data in a VPN secure tunnel to an internal address of the mobile node to create VPN packaged data and tunneling the VPN packaged data to a current address of the mobile node **(See page 3 paragraphs 26-28 and Figure 4 of Adrangi et al. for reference to using a VPN gateway 225 to package data in a secure VPN tunnel to an internal address of the mobile node 140 and tunneling the data to a care of address of the mobile node 140)**. Adrangi et al. further discloses packaging the collected data in an IP-in-IP tunnel and sending it to a VPN device for VPN encryption and tunneling the VPN packaged data to the current address of the mobile node **(See page 4 paragraphs 29-30 and Figure 6 of Adrangi et al. for reference to packaging the data in an IPSEC tunnel, which is an IP-in-IP tunnel, and sending it to a VPN gateway 225 for VPN encryption before sending the packet to the care of address of the mobile node)**. Adrangi et al. does not disclose that the HA is configured to notify the PHA of the mobile node.

With respect to claim 15, Liu et al. ('295), in the field of communications, discloses a home agent that notifies a proxy home agent of a mobile node **(See page 3 paragraphs 34-35 and Figure 1A of Liu et al. ('295) for reference to a mobile connectivity system 100 that includes a mobile node 120, an MIP proxy 102,**

which acts as a home agent, and a home agent 112, which acts as a proxy home agent, and for reference to the MIP proxy 102 sending a registration request, which is a notification of the mobile node 120, on behalf of the mobile node 120 to the home agent 112). Having the HA configured to notify the PHA of the mobile node has the advantage of allowing a mobile node to roam from network to network without requiring the mobile node to set up a new security binding each time the mobile node changes networks (See page 5 paragraph 53 of Liu et al. ('295) for reference to this advantage as well as other advantages).

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Liu et al. ('295), to combine having the HA configured to notify the PHA of the mobile node, as suggested by Liu et al. ('295), with the system and method of Adrangi et al., with the motivation being to allow a mobile node to roam from network to network without requiring the mobile node to set up a new security binding each time the mobile node changes networks.

With respect to claim 16, Adrangi et al. discloses that the VPN secure tunnel follows the IP security protocol **(See page 2 paragraph 22 of Adrangi et al. for reference to using IPSec protocol)**.

With respect to claim 17, Adrangi et al. discloses that the tunneling of the VPN packaged data to the external mobile node occurs according to the IP mobility protocol **(See page 1 paragraph 3 of Adrangi et al. for reference to using mobile IP standards)**.

With respect to claim 20, the combination of Adrangi et al. and Liu et al. discloses all the limitations of claim 15 as shown above and Adrangi et al. also discloses a computer software product comprising instruction that cause an electronic device to perform the method **(See page 4 paragraphs 33-34 of Adrangi et al. for reference to the devices of the system of Adrangi et al. being embodied as data processing devices including software comprising instructions that the devices of the system use to perform the method of Adrangi et al.)**.

7. Claims 1-5, 7-10, 14, 19, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adrangi et al. in view of Liu et al. ('295) and Liu et al ('900) as applied to claims 1-4, 7-10, 14, and 19 above, and further in view of Le et al. (U.S. Publication US 2003/0093553 A1).

With respect to claim 1, Adrangi et al. discloses a system for providing secure mobile connectivity that implements Mobile IP Home Agent functionality via distributed components **(See the abstract of Adrangi et al. for reference to a system providing secure mobile roaming using distributed components)**. Adrangi et al. also discloses a mobile node belonging to a home network located within a secure network with the mobile node having a network interface configured to communicate with other nodes **(See page 2 paragraphs 20-22 and Figure 3 of Adrangi et al. for reference to a mobile node 140 having an interface to communicate with other nodes belonging to corporate intranet 100, which is a home network for mobile node 140 and is also a secure network)**. Adrangi et al. further discloses that the mobile node

has only one security association and only one mobility binding with a Home Agent for the Mobile IP Home Agent functionality **(See page 3 paragraphs 23-28 and Figures 3-4 of Adrangi et al. for reference to a mobile node creating a single security association, an IPSec tunnel, with a VPN 225 and for reference to a mobile node having one mobility bind, the care-of address COAx, which is the mobile node's address on the external network)**. Adrangi et al. also discloses a Proxy Home Agent connected to the home network and located within the secure network wherein the PHA is configured to provide a proxying functionality **(See page 2 paragraph 20, page 3 paragraph 28, and Figures 3-5 of Adrangi et al. for reference to home agent 300, which is a Proxy Home Agent providing Mobile IP Home Agent functionality, located within the corporate intranet 100, and for reference to home agent 300 performing a proxy functionality by determining that a mobile node is not in its home location and forwarding the packet to the VPN gateway 225 based on this determination)**. Adrangi et al. further discloses a Home Agent located outside of the secure network wherein the HA is configured to provide a signaling and tunneling functionality **(See page 2 paragraph 20, page 3 paragraph 38 and Figures 3-5 of Adrangi et al. for reference to home agent 305, which provides Mobile IP Home Agent functionality, located outside the corporate intranet 100 and for reference to home agent 305 providing a signaling and tunneling functionality by tunneling packets to a mobile node 140 based on the care-of address, COAx, of the mobile node)**. Adrangi et al. also discloses a VPN gateway located outside the secure network and configured to work in conjunction with the HA **(See page 2 paragraph 20 and**

Figure 3 of Adrangi et al. for reference to VPN gateway 225 located outside the corporate intranet 100 and configured to work with the home agent 305). Adrangi et al. further discloses a DMZ located outside the secure network wherein the VPN gateway and the HA reside in the DMZ **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to corporate DMZ 210 that is located outside the secure network and includes the VPN gateway 225 and home agent 305)**. Adrangi et al. also discloses a first firewall between the secure network and the DMZ **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to inner firewall 15, which is a first firewall located between the corporate intranet 100 and the DMZ 210)**. Adrangi et al. does not disclose that the HA is configured to notify the PHA of the mobile node. Adrangi et al. also does not specifically disclose that the first firewall is configured to deny communications from the DMZ with a source address in a known range. Adrangi et al. further does not disclose the mobile node having a permanent address in a known range.

With respect to claim 19, Adrangi et al. discloses a system for secure mobile connectivity that implements Mobile IP Home Agent functionality via distributed components **(See the abstract of Adrangi et al. for reference to a system providing secure mobile roaming using distributed components)**. Adrangi et al. also discloses a means for establishing a Proxy Home Agent located within the secure network to monitor data directed to the mobile node **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 300, which is a Proxy Home Agent providing Mobile IP Home Agent functionality, located within corporate**

intranet 100, which is a secure network). Adrangi et al. further discloses a means for establishing a Home Agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 305, which provides Mobile IP Home Agent functionality, located outside the corporate intranet 100, for reference a mobile node creating a single security association, an IPSec tunnel, and for reference to a mobile node having one mobility bind, the care-of address COAx, which is the mobile node's address on the external network)**. Adrangi et al. also discloses a means for collecting data directed to the mobile node **(See page 2 paragraph 20 to page 3 paragraph 25 of Adrangi et al. for reference to both home agent 300 and home agent 305 being used to collect and route data directed to the mobile node 140)**. Adrangi et al. further discloses a means for packaging the collected data in a VPN secure tunnel to an internal address of the mobile node to create VPN packaged data and a means for tunneling the VPN packaged data to a current address of the mobile node **(See page 3 paragraphs 26-28 and Figure 4 of Adrangi et al. for reference to using a VPN gateway 225 to package data in a secure VPN tunnel to an internal address of the mobile node 140 and tunneling the data to a care of address of the mobile node 140)**. Adrangi et al. also discloses a means for the Home Agent to communicate to the PHA that the mobile node has either moved outside its home network or has come back to its home network **(See pages 2-3 paragraphs 20-25 of Adrangi et al. for reference to the home agents 300 and 305 updating the current location of the mobile node 140 by**

storing a current care of address of the mobile node that indicates the location of the node). Adrangi et al. further discloses a means for enabling the PHA to create and remove a proxy ARP entry for a permanent address associated with the mobile node **(See page 3 paragraph 25 of Adrangi et al. for reference to home agent 300 creating and removing care of address entries, which are proxy ARP entries for a permanent address associated with the mobile node 140)**. Adrangi et al. further discloses a DMZ located outside the secure network wherein the VPN gateway and the HA reside in the DMZ **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to corporate DMZ 210 that is located outside the secure network and includes the VPN gateway 225 and home agent 305)**. Adrangi et al. also discloses a firewall between the secure network and the DMZ **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to inner firewall 15, which is a first firewall located between the corporate intranet 100 and the DMZ 210)**. Adrangi et al. does not disclose that the HA is configured to notify the PHA of the mobile node. Adrangi et al. also does not specifically disclose that the firewall is configured to deny communications from the DMZ with a source address in a known range.

With respect to claims 1 and 19, Liu et al. ('295), in the field of communications, discloses a home agent that notifies a proxy home agent of a mobile node **(See page 3 paragraphs 34-35 and Figure 1A of Liu et al. ('295) for reference to a mobile connectivity system 100 that includes a mobile node 120, an MIP proxy 102, which acts as a home agent, and a home agent 112, which acts as a proxy home agent, and for reference to the MIP proxy 102 sending a registration**

request, which is a notification of the mobile node 120, on behalf of the mobile node 120 to the home agent 112). Having the HA configured to notify the PHA of the mobile node has the advantage of allowing a mobile node to roam from network to network without requiring the mobile node to set up a new security binding each time the mobile node changes networks (See page 5 paragraph 53 of Liu et al. ('295) for reference to this advantage as well as other advantages).

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Liu et al. ('295), to combine having the HA configured to notify the PHA of the mobile node, as suggested by Liu et al. ('295), with the system and method of Adrangi et al., with the motivation being to allow a mobile node to roam from network to network without requiring the mobile node to set up a new security binding each time the mobile node changes networks.

With respect to claim 9, the combination of Adrangi et al. and Liu et al. ('295) does not disclose a firewall dropping packets having a source address in a known range.

With respect to claim 14, Adrangi et al. discloses a firewall coupled to the secure network and the VPN gateway **(See page 2 paragraph 20 of Adrangi et al. for reference to inner firewall 15 coupled to both the corporate intranet 100 and the VPN gateway 225)**. The combination of Adrangi et al. and Liu et al. ('295) does not disclose dropping packets having a source address in a known range.

With respect to claims 1, 9, 14, and 19, Liu et al. ('900), in the field of communications, discloses a firewall dropping packets having a source address in a

known range **(See page 2 paragraph 19 of Liu et al. for reference to maintaining an ALC table 104 that is used to store address and ranges of address and a field indicating that the address or range of address should be dropped by a firewall)**. Using a firewall that drops packets having a source address in a known range has the advantage of allowing better control of the packets that are allowed to enter a secure network to protect against malicious packets.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Liu et al. ('900), to combine using a firewall that drops packets having a source address in a known range, as suggested by Liu et al. ('900), with the system and method of Adrangi et al. and Liu et al. ('295), with the motivation being to allow better control of the packets that are allowed to enter a secure network to protect against malicious packets.

With respect to claims 5 and 21, Adrangi et al. discloses a second firewall between the DMZ and an external network **(See page 20 paragraph 20 and Figure 3 of Adrangi et al. for reference to outer firewall 20, which is a second firewall located between the DMZ 210 and an external network 205)**. The combination of Adrangi et al., Liu et al. ('295) and Liu et al. ('900) does not disclose the mobile node having a permanent address in a known range.

With respect to claims 1, 5, 19, and 21, Le et al., in the field of communications, discloses a mobile node having a permanent address in a known range **(See page 5 paragraphs 74-75 of Le et al. for reference to a mobile terminal node being identified by a permanent address, with addresses being within a**

known range useable in a network). A mobile node having a permanent address in a known range has the advantage of allowing better control over network access since a range of addresses assigned to mobile nodes is known by the network.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Le et al., to combine a mobile node having a permanent address in a known range, as suggested by Le et al., with the system and method of Adrangi et al., Liu et al. ('295), and Liu et al. ('900), with the motivation being to allow better control over network access since a range of addresses assigned to mobile nodes is known by the network.

With respect to claim 2, Adrangi et al. discloses that the VPN gateway and the HA are located within a single device within a DMZ **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 305 and VPN gateway 225 being located on a single processing device within a corporate DMZ 210)**.

With respect to claim 3, Adrangi et al. discloses a firewall coupled to the secure network and the VPN gateway **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to inner firewall 15 and outer firewall 20 being coupled to the corporate intranet 100 and the VPN gateway 225)**.

With respect to claim 4, Adrangi et al. discloses that the HA is a separate devices from the VPN gateway **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to the home agent 305 being implemented on an independent processing device within corporate DMZ 210, meaning the home agent 305 is a separate device from VPN gateway 225)**.

With respect to claim 7, Adrangi et al. discloses a DMZ comprising a first router coupled to a second router that is coupled to the firewall with the VPN gateway couple to the first router and the firewall and the HA coupled to the router **(See page 2 paragraph 20 of Adrangi et al. for reference to VPN gateway 225, which acts as a first router by routing packets, for reference to the VPN gateway 225 being coupled to the home agent 305, which acts as a second router by routing packets, and for reference to the VPN gateway 225 and the home agent 305 being coupled to firewalls 15 and 20)**.

With respect to claim 8, Adrangi et al. discloses that packets from the MN destined towards nodes inside the secure network first go to the HA and then to the VPN gateway that is configured to forward the packets through the firewall to the secure network **(See page 3 paragraph 27 and Figure 4 of Adrangi et al. for reference to packets sent from MN 140 to CN 310, which is a node inside of the corporate network 100, being first sent to home agent 305 and then to VPN gateway 225, which sends the packets through the firewall to CN 310)**.

With respect to claim 10, Adrangi et al. discloses that a router is directly connected to a firewall and the VPN gateway and the HA are connected to a different interface of the router and the firewall **(See page 2 paragraph 20, page 3 paragraph 28, page 4 paragraph 32 and Figure 3 of Adrangi et al. for reference to home agents 305 and 300 both acting as routers to route packets between networks and for reference to VPN gateway 225 being connected to an inner firewall 15 and an outer firewall 20 and for reference to the VPN gateway 225 and the home agent**

305 being separate devices meaning that their connections to the firewalls 15 and 20 are through separate interfaces).

Allowable Subject Matter

8. Claim 6 is objected to as being dependent upon a rejected base claim, as well as for the other reasons state above, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims as well as being amended to fix the above mentioned problems.

9. Claims 11-13 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

10. The following is a statement of reasons for the indication of allowable subject matter:

Claim 6 would be allowable since none of the prior art of record discloses or renders obvious the limitation of the virtual private network gateway having a direct connection to an internal interface of the first firewall such that the first firewall considers the virtual private network gateway transmitted data as internal to the secure network.

Claim 11 would be allowable since none of the prior art of record discloses or renders obvious the limitation of dropping packets with a source address outside a

known address ranged that are received on an internal interface and dropping packets with a source address within the known address range that are received on an external interface.

Claims 12 and 13 would be allowable since they depend on claim 11.

Response to Arguments

11. Applicant's arguments filed 6/26/08 have been fully considered but they are not persuasive.

Regarding Applicant's argument that claim 15 has been amended to overcome the rejection under 35 U.S.C. 112 second paragraph, the Examiner respectfully disagrees. Claim 15 has not been amended.

Regarding Applicant's argument that claims 1 and 19 have been amended to include subject previously indicated as allowable, the Examiner respectfully disagrees. Although some language from previously indicated allowable claim 6 has been added to claims 1 and 19, not all the indicated allowable language has been added to these claims. Thus, claims 1 and 19 have been rejected, as shown above. It is recommended that all the indicated allowable subject matter from previous claim 6 be included in independent claims 1 and 19, such that they are allowable.

Regarding Applicant's argument that Adrangi et al. does not teach or suggest a home agent creating only one security association and only one mobility binding with a mobile node as recited in independent claim 15, the Examiner respectfully disagrees.

Applicant argues that Adrangi et al. discloses multiple mobility bindings because Adrangi et al. teaches multiple possible mobility bindings (multiple COAs) being used as the MN 140 moves from one subnet to another. Adrangi et al. never discloses using multiple COAs at the same time and merely discloses that the COA is updated as the MN moves in the network. Thus, only one COA (one mobility binding) is established between the MN and the home agent 305 at any time. The claim language states that the mobile node has only one security association and only one mobility binding with a home agent. Since Adrangi et al. never discloses multiple COAs used at the same time, Adrangi et al. discloses the mobile node only having one mobility binding with the home agent at any given time.

Regarding Applicant's argument that Adrangi et al. does not disclose "packaging the collected data in an internet-protocol-in-internet-protocol tunnel and sending it to a VPN device for VPN encryption and tunneling the VPN packaged data to the current address of the mobile node", the Examiner respectfully disagrees. Adrangi et al. discloses packaging data in an IPSEC tunnel, which is an IP-in-IP tunnel as known in the art, and sending it to a VPN gateway 225 for VPN encryption before sending the packet to the care of address of the mobile node (See page 4 paragraphs 29-30 and Figure 6 of Adrangi et al.).

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON E. MATTIS whose telephone number is (571)272-3154. The examiner can normally be reached on M-F 8AM-5:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Firmin Backer can be reached on (571)272-6703. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jason E Mattis
Examiner
Art Unit 2416

JEM

/Huy D. Vu/
Supervisory Patent Examiner, Art Unit 2616